Using Backup and Restore

Backup and restoration is an essential part of any system maintenance plan. While each organization's backup plan is highly individualized, the FireSIGHT System provides a mechanism for archiving data so that data from a Defense Center or physical managed device can be restored in case of disaster.

Note the following limitations about backup and restore:

- Backups are valid only for the product version on which you create them.
- Backups do not include captured file data.
- You cannot create or restore backup files for virtual managed devices, Cisco NGIPS for Blue Coat X-Series, or Cisco ASA with FirePOWER Services. To back up all event data, perform a backup of the managing Defense Center.
- You can restore a backup onto a replacement appliance only if the two appliances are the same model and are running the same version of the FireSIGHT System software.

Caution Do not use the backup and restore process to copy the configuration files between managed devices. The configuration files include information that uniquely identifies a device and cannot be shared.

Caution If you applied any intrusion rule updates, those updates are not backed up. You need to apply the latest rule update **after** you restore.

You can save backup files to the appliance or to your local computer. Additionally, if you are using a Defense Center, you can use remote storage as detailed in Managing Remote Storage, page 64-15.

Caution Never insert a USB drive into any USB port on a 3D9900. Additionally, remove any device with external storage (for example, a KVM switch with external storage) from a 3D9900 before upgrading or restoring the device.

See the following sections for more information:

- See Creating Backup Files, page 70-2 for information about creating backup files for Defense Centers and physical managed devices.
- See Creating Backup Profiles, page 70-6 for information about creating backup profiles that you can use later as templates for creating backups.
- See Uploading Backups from a Local Host, page 70-7 for information about uploading backup files from a local host.

- See Restoring the Appliance from a Backup File, page 70-7 for information about how to restore a backup file to the appliance.

Creating Backup Files

License: Any

Supported Devices: Any except virtual, X-Series, and ASA FirePOWER

Supported Defense Centers: Any

You can perform backups of physical managed devices from the devices themselves, backups of physical managed devices from their managing Defense Center, and backups of Defense Centers. The system backs up different data depending on the type of backup you perform. Note that the system does **not** back up captured file data. Use the following table to determine what kind of backup you want to perform.

Table 70-1 Data Stored by Backup Type

Backup type	Includes configuration data?	Includes event data?	Includes unified files?
Defense Center	Yes	Yes	No
Physical managed device, performed from the device itself	Yes	No	No
Physical managed device, performed from the managing Defense Center	Yes	No	Yes

Note You **cannot** create or restore backup files for virtual managed devices, Cisco NGIPS for Blue Coat X-Series, or Cisco ASA with FirePOWER Services. To back up event data, perform a backup of the managing Defense Center.

To view and use existing system backups, go to the Backup Management page. You should periodically save a backup file that contains all of the configuration files required to restore the appliance, in addition to event data. You may also want to back up the system when testing configuration changes so that you can revert to a saved configuration if needed. You can choose to save the backup file on the appliance or on your local computer.

You cannot create a backup file if your appliance does not have enough disk space; backups may fail if the backup process uses more than 90% of available disk space. If necessary, delete old backup files, transfer old backup files off the appliance, or use remote storage.

As an alternative, or if your backup file is larger than 4GB, copy it via SCP to a remote host. Uploading a backup from your local computer does not work on backup files larger than 4GB because web browsers do not support uploading files that large. On Defense Centers, the backup file can be saved to a remote location; see Managing Remote Storage, page 64-15 for more information.

Note While your backup task is collecting discovery events, data correlation is temporarily suspended.

Note the following:

- Private keys associated with PKI objects are encrypted with a randomly generated key when stored on the appliance. If you perform a backup that contains private keys associated with PKI objects, the private keys are decrypted before being included in the unencrypted backup file. Store the backup file in a secure location.
- If you restore a backup that contains private key associated with PKI objects, the system encrypts the keys with a randomly generated key before storing them on the appliance.
- If you perform a backup, then delete reviewed intrusion events, your backup restores the deleted intrusion events but does not restore their reviewed status. You view those restored intrusion events under Intrusion Events, not under Reviewed Events. See Reviewing Intrusion Events, page 41-16.
- If you restore a backup that contains intrusion event data on an appliance that already contains that data, duplicate events are created. To avoid this, restore intrusion event backups only on appliances without prior intrusion event data.

Caution If you configured any interface associations with security zones, these associations are not backed up. You must reconfigure them after you restore. For more information, see Working with Security Zones, page 3-39.

To create a backup file of a Defense Center:

Access: Admin/Maint

Step 1 Select **System > Tools > Backup/Restore**.

The Backup Management page appears.

Step 2 Click **Defense Center Backup**.

The Create Backup page appears.

Step 3 In the **Name** field, type a name for the backup file. You can use alphanumeric characters, punctuation, and spaces.

Step 4 On Defense Centers, you have two further options:

- To archive the configuration, select **Back Up Configuration**.
- To archive the entire event database, select **Back Up Events**.

Step 5 Optionally, to be notified when the backup is complete, select the **Email** check box and type your email address in the accompanying text box.

Note To receive email notifications, you must configure a relay host as described in Configuring a Mail Relay Host and Notification Address, page 63-18.

Step 6 Optionally, on Defense Centers, to use secure copy (`SCP`) to copy the backup archive to a different machine, select the **Copy when complete** check box, then type the following information in the accompanying text boxes:

- in the **Host** field, the hostname or IP address of the machine where you want to copy the backup
- in the **Path** field, the path to the directory where you want to copy the backup
- in the **User** field, the user name you want to use to log into the remote machine

- in the **Password** field, the password for that user name
  If you prefer to access your remote machine with an SSH public key instead of a password, you must copy the contents of the **SSH Public Key** field to the specified user's `authorized_keys` file on that machine.

With this option cleared, the system stores temporary files used during the backup on the remote server; temporary files are **not** stored on the remote server when this option is selected.

Tip Cisco recommends that you periodically save backups to a remote location so the appliance can be restored in case of system failure.

Step 7 You have the following options:

- To save the backup file to the appliance, click **Start Backup**.

  The backup file is saved in the `/var/sf/backup` directory. You can direct the backup file to a remote location; see Managing Remote Storage, page 64-15.

  When the backup process is complete, you can view the file on the Restoration Database page. For information about restoring a backup file, see Restoring the Appliance from a Backup File, page 70-7.

- To save this configuration as a backup profile that you can use later, click **Save As New**.

  You can modify or delete the backup profile by selecting **System > Tools > Backup/Restore**, then clicking **Backup Profiles**. See Creating Backup Profiles, page 70-6 for more information.

To create a backup file of a physical managed device from the device itself:

Access: Admin/Maint

Step 1 Select **System > Tools > Backup/Restore**.

The Device Backups page appears.

Step 2 Click **Device Backup**.

The Create Backup page appears.

Step 3 In the **Name** field, type a name for the backup file. You can use alphanumeric characters, punctuation, and spaces.

Step 4 Optionally, to be notified when the backup is complete, select the **Email** check box and type your email address in the accompanying text box.

Note To receive email notifications, you must configure a relay host as described in Configuring a Mail Relay Host and Notification Address, page 63-18.

Step 5 Optionally, to use secure copy (`SCP`) to copy the backup archive to a different machine, select the **Copy when complete** check box, then type the following information in the accompanying text boxes:

- in the **Host** field, the hostname or IP address of the machine where you want to copy the backup
- in the **Path** field, the path to the directory where you want to copy the backup
- in the **User** field, the user name you want to use to log into the remote machine

- in the **Password** field, the password for that user name
  If you prefer to access your remote machine with an SSH public key instead of a password, you must copy the contents of the **SSH Public Key** field to the specified user's `authorized_keys` file on that machine.

With this option cleared, the system stores temporary files used during the backup on the remote server; temporary files are **not** stored on the remote server when this option is selected.

Tip Cisco recommends that you periodically save backups to a remote location so the appliance can be restored in case of system failure.

Step 6 You have the following options:

- To save the backup file to the appliance, click **Start Backup**.

  The backup file is saved in the `/var/sf/backup` directory. On Defense Centers, you can direct the backup file to a remote location; see Managing Remote Storage, page 64-15.

  When the backup process is complete, you can view the file on the Restoration Database page. For information about restoring a backup file, see Restoring the Appliance from a Backup File, page 70-7.
- To save this configuration as a backup profile that you can use later, click **Save As New**.

  You can modify or delete the backup profile by selecting **System > Tools > Backup/Restore**, then clicking **Backup Profiles**. See Creating Backup Profiles, page 70-6 for more information.

To create a backup file of a physical managed device from its managing Defense Center:

Access: Admin/Maint

Step 1 Select **System > Tools > Backup/Restore**.

The Backup Management page appears.

Step 2 Click **Managed Device Backup**.

The Create Backup page appears.

Step 3 In the **Managed Devices** field, select one or more managed devices. Use the Shift or Ctrl keys to select multiple managed devices.

Step 4 To include unified files in addition to configuration data, select the **Include All Unified Files** check box.

Step 5 To save the backup file on the Defense Center, select the **Retrieve to Defense Center** check box. To save each device's backup file on the device itself, leave this check box unselected.

Note If you select **Retrieve to Defense Center** and your Defense Center is configured for remote storage of backups, the device backup file will be saved to the configured remote location, not the Defense Center itself.

Step 6 Click **Start Backup**.

A success message appears and the backup task is created.

The backup file is saved in the `/var/sf/backup` directory. Using the Defense Center, you can direct the backup file to a remote location; see Managing Remote Storage, page 64-15.

When the backup process is complete, you can view the file on the Restoration Database page. For information about restoring a backup file, see Restoring the Appliance from a Backup File, page 70-7.

Step 7 Optionally, to save this configuration as a backup profile that you can use later, click **Save As New**.

You can modify or delete the backup profile by selecting **System > Tools > Backup/Restore**, then clicking **Backup Profiles**. See Creating Backup Profiles, page 70-6 for more information.

Creating Backup Profiles

License: Any

Supported Devices: Any except virtual, X-Series, and ASA FirePOWER

Supported Defense Centers: Any

You can use the Backup Profiles page to create backup profiles that contain the settings that you want to use for different types of backups. You can later select one of these profiles when you back up the files on your appliance.

Tip When you create a backup file as described in Creating Backup Files, page 70-2, a backup profile is automatically created.

To create a backup profile:

Access: Admin/Maint

Step 1 Select **System > Tools > Backup/Restore**.

The Backup Management page appears.

Step 2 Click the **Backup Profiles** tab.

The Backup Profiles page appears with a list of existing backup profiles.

Tip You can click the edit icon ( ) to modify an existing profile or click the delete icon ( ) to delete a profile from the list.

Step 3 Click **Create Profile**.

The Create Backup page appears.

Step 4 Type a name for the backup profile. You can use alphanumeric characters, punctuation, and spaces.

Step 5 Configure the backup profile according to your needs.

See Creating Backup Files, page 70-2 for more information about the options on this page.

Step 6 Click **Save As New** to save the backup profile.

The Backup Profiles page appears and your new profile appears in the list.

Uploading Backups from a Local Host

License: Any

Supported Devices: Series 2 and Series 3

Supported Defense Centers: Any

If you download a backup file to your local host using the download function described in the Backup Management table, you can upload it to a Defense Center.

If your backup file contains PKI objects, private keys associated with internal CA and internal certificate objects are re-encrypted on upload with a randomly generated key.

Tip You cannot upload a backup larger than 4GB from your local host because web browsers do not support uploading files that large. As an alternative, copy the backup via SCP to a remote host and retrieve it from there. On Defense Centers, the backup file can be saved to and retrieved from a remote location; see Managing Remote Storage, page 64-15.

To upload a backup from your local host:

Access: Admin/Maint

Step 1 Select **System > Tools > Backup/Restore**.

The Backup Management page appears.

Step 2 Click **Upload Backup.**

The Upload Backup page appears.

Step 3 Click **Browse** and navigate to the backup file you want to upload.

After you select the file to upload, click **Upload Backup**.

Step 4 Click **Backup Management** to return to the Backup Management page.

The backup file is uploaded and appears in the backup list. After the Defense Center appliance verifies the file integrity, refresh the Backup Management page to reveal detailed file system information.

Restoring the Appliance from a Backup File

License: Any

Supported Devices: Series 2 and Series 3

Supported Defense Centers: Any

You can restore the appliance from backup files using the Backup Management page. To restore a backup, the VDB version in the backup file must match the current VDB version on your appliance. After you complete the restoration process, you **must** apply the latest Sourcefire Rule Update.

Caution Do not restore backups created on virtual Defense Centers to physical Defense Centers — this may stress system resources. If you must restore a virtual backup on a physical Defense Center, contact Support.

If your backup file contains PKI objects, private keys associated with internal CA and internal certificate objects are reencrypted on upload with a randomly generated key.

If you use local storage, backup files are saved to `/var/sf/backup`, which is listed with the amount of disk space used in the `/var` partition at the bottom of the Backup Management page. On Defense Centers, select **Remote Storage** at the top of the Backup Management page to configure remote storage options; then, to enable remote storage, select the **Enable Remote Storage for Backups** check box on the Backup Management page. If you use remote storage, the protocol, backup system, and backup directory are listed at the bottom of the page.

Note If you add licenses after a backup has completed, these licenses will not be removed or overwritten if this backup is restored. To prevent a conflict on restore, remove those licenses before restoring the backup, noting where the licenses were used, and add and reconfigure them after restoring the backup. If a conflict occurs, contact Support.

The following table describes each column and icon on the Backup Management page.

Table 70-2 Backup Management

Functionality	Description
System Information	The originating appliance name, type, and version. Note that you can only restore a backup to an identical appliance type and version.
Date Created	The date and time that the backup file was created
File Name	The full name of the backup file
VDB Version	The build of the vulnerability database (VDB) running on the appliance at the time of backup.
Location	The location of the backup file
Size (MB)	The size of the backup file, in megabytes
Events?	"Yes" indicates the backup includes event data
View	Click the name of the backup file to view a list of the files included in the compressed backup file.
Restore	Click with the backup file selected to restore it on the appliance. If your VDB version does not match the VDB version in the backup file, this option is disabled.
Download	Click with the backup file selected to save it to your local computer.
Delete	Click with the backup file selected to delete it.
Move	On a Defense Center, when you have a previously created local backup selected, click to send the backup to the designated remote backup location.

To restore the appliance from a backup file:

Access: Admin

Step 1 Select **System > Tools > Backup/Restore**.

The Backup Management page appears.

Step 2 To view the contents of a backup file, click the name of the file.

The manifest appears, listing the name of each file, its owner and permissions, and its file size and date.

Step 3 Click **Backup Management** to return to the Backup Management page.

Step 4 Select the backup file that you want to restore and click **Restore**.

The Restore Backup page appears.

Note that if the VDB version in the backup does not match the VDB version currently installed on your appliance, the **Restore** button is grayed out.

Caution This procedure overwrites all configuration files and, on the managed device, all event data.

Step 5 To restore files, select either or both:

- **Replace Configuration Data**
- **Restore Event Data**

Note Note that, when you restore the configuration of a managed device from a backup file, any device configuration changes you made from the device's managing Defense Center will also be restored, even changes you made after you created that backup file.

Step 6 Click **Restore** to begin the restoration.

The appliance is restored using the backup file you specified.

Step 7 Reboot the appliance.

Step 8 Apply the latest Sourcefire Rule Update to reapply rule updates.

Step 9 Reapply any access control, intrusion, network discovery, health, and system policies to the restored system.